PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G11B 20/00, G06F 1/00

A1

(11) Internationale Veröffentlichungsnummer: WO 96/29699

(43) Internationales Veröffentlichungsdatum: 26. September 1996 (26.09.96)

(21) Internationales Aktenzeichen: PCT/EP96/01175

(22) Internationales Anmeldedatum: 19. März 1996 (19.03.96)

(30) Prioritätsdaten:
195 12 218.6 22. März 1995 (22.03.95) DE

(71) Anmelder (*für alle Bestimmungsstaaten ausser US*): MEILLER COMCARD GMBH [DE/DE]; Hammerbrücker Strasse 3, D-08223 Falkenstein (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder (*nur für US*): LENDER, Friedwart [DE/DE]; Georg-Strobel-Strasse 73, D-90489 Nürnberg (DE). HORSTER, Patrick [DE/DE]; Schervier Strasse 19, D-50226 Frechen (DE).

(74) Anwälte: TERGAU, Enno usw.; Mögeldorfer Hauptstrasse 51, D-90482 Nürnberg (DE).

(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO Patent (KE, LS, MW, SD, SZ, UG), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

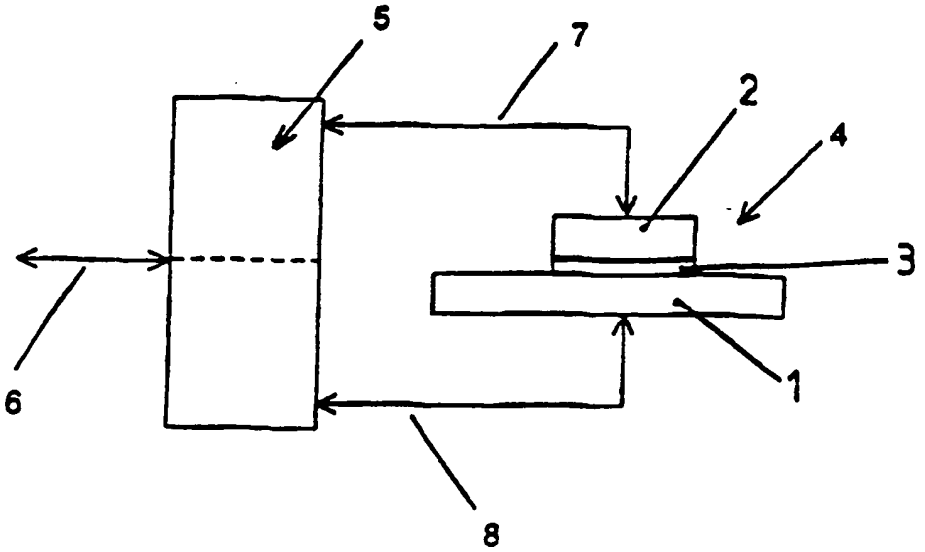
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: PROTECTION DEVICE FOR DATA CARRIERS AND AN INTERACTIVE DEVICE WHICH CO-OPERATES WITH THE PROTECTION DEVICE TO PREVENT UNAUTHORISED USE

(54) Bezeichnung: SCHUTZVORRICHTUNG FÜR DATENTRÄGER UND DAMIT ZUSAMMENWIRKENDE INTERAKTIONSEINRICHTUNG GEGEN UNERLAUBTE NUTZUNG

(57) Abstract

The invention concerns a device for protecting portable storage mediums used as data carriers (1) against unauthorised use of data and/or for similarly protecting an interactive device (5) which communicates with the data carrier. The data carrier (1) is physically coupled (3) to at least one security module (2). The security module (2) and interactive device (5), as integral parts of the protective device, co-operate in such a way that a user's access to the data carrier (1) and/or the interactive device (5) in a way useful is conditional on an exchange of mutually co-ordinated data between the security module (2) and interactive device (5).



(57) Zusammenfassung

Die Erfindung betrifft eine Vorrichtung zum Schutz von transportablen Speichermedien als Datenträger (1) gegen unerlaubte Datennutzung und/oder zum Schutz einer mit dem Datenträger kommunizierenden Interaktionseinrichtung (5) gegen unerlaubte Nutzung. Der Datenträger (1) ist mit mindestens einem Sicherheitsmodul (2) physikalisch gekoppelt (3). Der Sicherheitsmodul (2) und die Interaktionseinrichtung (5) als Bestandteile der Schutzvorrichtung wirken derart zusammen, daß nur in Abhängigkeit eines Austausches von aufeinander abgestimmten Informationen zwischen dem Sicherheitsmodul (2) und der Interaktionseinrichtung (5) auf den Datenträger (1) und/oder auf die Interaktionseinrichtung (5) in einer für einen Benutzer auswertbaren Form zugreifbar ist.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AM	Armenien	GB	Vereinigtes Königreich	MX	Mexiko
AT	Österreich	GE	Georgien	NE	Niger
AU	Australien	GN	Guinea	NL	Niederlande
BB	Barbados	GR	Griechenland	NO	Norwegen
BE	Belgien	HU	Ungarn	NZ	Neuseeland
BF	Burkina Faso	IE	Irland	PL	Polen
BG	Bulgarien	IT	Italien	PT	Portugal
BJ	Benin	JP	Japan	RO	Rumänien
BR	Brasilien	KE	Kenya	RU	Russische Föderation
BY	Belarus	KG	Kirgisistan	SD	Sudan
CA	Kanada	KP	Demokratische Volksrepublik Korea	SE	Schweden
CF	Zentrale Afrikanische Republik	KR	Republik Korea	SG	Singapur
CG	Kongo	KZ	Kasachstan	SI	Slowenien
CH	Schweiz	LI	Liechtenstein	SK	Slowakei
CI	Côte d'Ivoire	LK	Sri Lanka	SN	Senegal
CM	Kamerun	LR	Liberia	SZ	Swasiland
CN	China	LK	Litauen	TD	Tschad
CS	Tschechoslowakei	LU	Luxemburg	TG	Togo
CZ	Tschechische Republik	LV	Lettland	TJ	Tadschikistan
DE	Deutschland	MC	Monaco	TT	Trinidad und Tobago
DK	Dänemark	MD	Republik Moldau	UA	Ukraine
EE	Estland	MG	Madagaskar	UG	Uganda
ES	Spanien	ML	Mali	US	Vereinigte Staaten von Amerika
FI	Finnland	MN	Mongolei	UZ	Usbekistan
FR	Frankreich	MR	Mauretanien	VN	Vietnam
GA	Gabon	MW	Malawi		

Beschreibung

Schutzvorrichtung für Datenträger und damit zusammenwirkende Interaktionseinrichtung gegen unerlaubte Nutzung

Werden Informationen auf einen Datenträger geschrieben, so sind zur Realisierung der Unversehrtheit (Datenintegrität), Vertraulichkeit, Authentizität, Originalität und sonstiger Sicherheitsfunktionalitäten, wie beispielsweise der Personalisierung von Daten und der Identifikation des Datenträgers selbst bestimmte Mechanismen erforderlich. Zudem muß oft der Aspekt eines wie auch immer gearteten Datenschutzes berücksichtigt werden. Einige der bisher bekannten Anwendungen liegen im Bereich des Softwareschutzes (z.B. Kopieren, unautorisierte Nutzung, Virenschutz), des Transportschutzes (Vertraulichkeit, Authentizität, sichere Schlüsselhaltung) und der eindeutigen Zuordnung von Daten bzw. Datenträgern zu Personen und/oder zu Geräten (Personalisierung, gegenseitige Authentifikation).

Durch klassische Datenträger alleine sind die aufgeführten Anwendungen nicht mit der erforderlichen Sicherheit zu realisieren.

Aus DE 44 19 115 A1 ist es bekannt, zum Schutz einer Software vor unautorisierter Benutzung eine Chipkarte in Verbindung mit einer Chipkarten-Lesevorrichtung und einem Prüfprogramm einzusetzen. Die spezielle Ausgestaltung der Lesevorrichtung und deren physikalische und logische Kopplung mit einem Rechnersystem sind jedoch regelmäßig mit einem hohen Aufwand verbunden. Außerdem sind weitere Bauteile und physikalische Verbindungen notwendig, um die Kommunikation zwischen den Lesevorrichtungen der Chipkarte und der Software herzustellen. Diese Kommunikationsverbindungen sind jedoch anfällig gegen ein unerlaubtes Anzapfen der Sicherheitsinformationen.

Der Erfindung liegt die Aufgabe zugrunde, mit geringem Aufwand eine große Sicherheit von Datenträgern und damit zusammenwirkenden Kommunikationseinrichtungen gegen unerlaubte Nutzung zu gewährleisten.

Diese Aufgabe wird durch die Merkmalskombination des Anspruches 1 gelöst.

Die erfindungsgemäße Schutzvorrichtung weist einen Sicherheitsmodul und eine mit dem Datenträger und dem Sicherheitsmodul zusammenwirkende Interaktionseinrich-

tung auf. Zwischen dem Sicherheitsmodul und der Interaktionseinrichtung findet ein Austausch von Informationen statt. Nur wenn bestimmte, aufeinander abgestimmte Informationen vom Sicherheitsmodul und/oder von der Interaktionseinrichtung gesendet oder empfangen werden, kann ein Benutzer auf die Daten des Datenträgers und/oder auf die Interaktionseinrichtung in einer für ihn auswertbaren Form zugreifen.

Durch den Austausch von aufeinander abgestimmten Informationen umfaßt die Schutzvorrichtung auch einen Entschlüsselungsschutz der auf dem Datenträger abgespeicherten Daten. So kann bei Nichtvorhandensein des dem Datenträger zugeordneten Sicherheitsmoduls der verschlüsselte Dateninhalt des Datenträgers zwar in herkömmlichen Lesegeräten ausgelesen bzw. kopiert werden, die für den Benutzer erforderliche Entschlüsselung des Dateninhalts zu dessen Auswertung findet jedoch bei registriertem Fehlen des Sicherheitsmoduls oder registriertem falschen Sicherheitsmodul nicht statt. Hierzu ist der aufeinander abgestimmte Informationsaustausch zwischen der Interaktionseinrichtung und dem Sicherheitsmodul notwendig. Analoge Anwendungsfälle sind für das Überschreiben der Daten des Datenträgers möglich.

Somit ist eine Interpretation bzw. eine Nutzung der Daten in einer für den Benutzer auswertbaren Form nur mittels eines zugehörigen Sicherheitsmoduls möglich.

Die erfindungsgemäße Schutzvorrichtung kann außerdem eine unautorisierte Benutzung der Interaktionseinrichtung selbst oder eines an die Interaktionseinrichtung angeschlossenen Rechnersystems vollständig oder teilweise verhindern. So versperrt die Interaktionseinrichtung einem Benutzer den Zugang zum Rechnersystem bzw. zu auf einer Festplatte abgelegten Daten oder zu Funktionen der Interaktionseinrichtung, wenn sie keinen oder nicht den richtigen Sicherheitsmodul auf dem Datenträger registriert.

Je nach Anwendungsfall wird ein Informationsaustausch vom Sicherheitsmodul oder von der Interaktionseinrichtung oder auch von beiden Komponenten kontrolliert. Für unterschiedliche Sicherheitsanforderungen sind also keine unterschiedlichen Lösungskonzepte erforderlich. Vielmehr können unterschiedliche Sicherheitsanforderungen durch das erfindungsgemäße Gesamtsystem verwirklicht werden. Abhängig vom jeweiligen Einsatzumfeld können die geforderten Sicherheitsmechanismen frei konfiguriert werden. Insbesondere können die eingangs genannten Anforderungen an Datenträger bzw. an den Datenzugriff realisiert werden.

Das vorgenannte Gesamtsystem ist gewissermaßen ein hybrides Gesamtsystem, welches durch hybride Datenträger und hybride Interaktionseinrichtungen gebildet ist. Beim hybriden Datenträger handelt es sich um ein transportables Speichermedium als Datenträger mit magnetischer, optischer oder sonstiger Datenspeicherfähigkeit, wie sie z.B. als Diskette, CD-ROM, optische Karte und Halbleiterspeicher bekannt sind. Der Sicherheitsmodul, der den Datenträger zu einem hybriden Datenträger ergänzt, ist ein verarbeitendes und/oder kommunizierendes Bauelement, welches nach festen oder ladbaren Regeln bzw. Algorithmen eine definierte Reaktion im Sicherheitsmodul selbst und/oder in der Interaktionseinrichtung erzeugt. Der Sicherheitsmodul ist z.B. als Speicher (mit oder ohne Sicherheitslogik), als Mikroprozessor, Mikrocontroller, Kryptoprozessor oder als Hologramm ausgebildet.

Der Datenträger kann mehrere, insbesondere auch unterschiedlich ausgebildete Sicherheitsmodule aufweisen.

Die hybride Interaktionseinrichtung weist auf den hybriden Datenträger abgestimmte Schreib-/Lese-Einheiten auf.

Bei dem hybriden Gesamtsystem wirkt der hybride Datenträger mit der hybriden Interaktionseinrichtung zusammen. Dieses Zusammenwirken wird durch die jeweiligen Sicherheitsanforderungen bestimmt und kann durch Konfiguration der Einzelkomponenten an die jeweilige Anwendung angepaßt werden. So kann die Sicherheitslogik zur Festlegung der Funktion des hybriden Gesamtsystems entweder im hybriden Datenträger oder in der hybriden Interaktionseinrichtung abgelegt sein. Der hybride Datenträger und die Interaktionseinrichtung können auch derart zusammenwirken, daß erst eine physikalische und/oder logische Verknüpfung des hybriden Datenträgers mit der Interaktionseinrichtung die Funktion des Gesamtsystems gewährleistet.

Vorteilhaft an dem hybriden Datenträger ist es, daß die räumliche Umrißform des Datenträgers unverändert bleiben kann, so daß herkömmliche Chassis von Interaktionseinrichtungen benutzbar und auch bekannte Bauteile dieser Interaktionseinrichtungen weiter verwendbar sind. Da die Interaktionseinrichtung sowohl mit dem Datenträger als auch mit dem Sicherheitsmodul kommuniziert, sind externe Kommunikationsverbindungen überflüssig. Auf die Sicherheitsinformationen kann deshalb nicht unautorisiert zugegriffen werden.

Gemäß Anspruch 2 ist die Sicherheit des Datenträgers gegen unerlaubten Datenzugriff weiter verbessert. Der Sicherheitsmodul ist einem bestimmten Datenträger durch die physikalische Kopplung eindeutig zugeordnet. Durch ein unautorisiertes Lösen des Sicherheitsmoduls vom Datenträger wird letzterer durch die feste oder zumindest schwer lösbare Kopplung beschädigt der zerstört. Der Datenträger ist deshalb unautorisiert nicht weiter verwendbar.

Die Maßnahme nach Anspruch 3 verbessert den unerlaubten Benutzungsschutz dadurch, daß der Datenträger und der Sicherheitsmodul erst beim Einsatz bzw. unmittelbar vor dem Einsatz physikalisch gekoppelt werden. So können Datenträger und Sicherheitsmodul auf getrennten Transportwegen versendet werden. Erst der Endkunde sorgt für die physikalische Kopplung.

Anspruch 4 berücksichtigt die physikalisch/konstruktiven Gegebenheiten des Chassis einer Interaktionseinrichtung, so daß das physikalische Zusammenwirken des hybriden Datenträgers mit herkömmlichen Chassis von Interaktionseinrichtungen weiter vereinfacht ist.

Gemäß Anspruch 5 wird die zunächst physikalische Kopplung des Sicherheitsmoduls mit dem Datenträger bei der Initialisierung des Sicherheitsmoduls durch eine logische Kopplung ergänzt. Diese logische Kopplung kann z.B. durch kryptographische Verfahren erfolgen.

Die logische Kopplung kann mittels der Interaktionseinrichtung oder durch eine im Datenträger integrierte logische Kopplung hergestellt werden.

Die logische Kopplung zwischen Sicherheitsmodul und Datenträger kann vorteilhaft auch dazu verwendet werden, die Funktion des hybriden Gesamtsystems festzulegen bzw. zu gewährleisten. Dabei kann der durch die logische Kopplung erzeugte Algorithmus vor dem Datenzugriff durch die Interaktionseinrichtung oder durch den hybriden Datenträger selbst gesteuert werden.

Die logische Kopplung zwischen Datenträger und Sicherheitsmodul ermöglicht eine eindeutige, unverwechselbare und sichere Identifikation des Datenträgers. Die logische Kopplung kann reversibel oder irreversibel sein. Sie wird entweder unmittelbar während

der Herstellung des hybriden Datenträgers oder zu einem späteren Zeitpunkt in diesen eingebracht. Die nachträgliche Einbringung der logischen Kopplung hat den Vorteil, daß der Informationsgehalt des Datenträgers ohne eine Initialisierung (z.B. durch Schlüsselvergabe) des Sicherheitsmoduls nicht rekonstruiert werden kann. Beispielsweise wird die in Lohnherstellung bereitgestellte Software verschlüsselt auf einer CD als Datenträger gepreßt, während der Software-Hersteller selbst den hybriden Datenträger - z.B. durch die Schlüsselvergabe - erst zu einem späteren Zeitpunkt aktiviert. Erst hierdurch wird der zunächst anonyme Datenträger eindeutig identifizierbar und die Daten werden erst dadurch nutzbar, d.h. für einen Benutzer interpretierbar.

Anspruch 7 unterstützt den Schutz eines Datenträgers gegen unautorisierte Datennutzung bzw. -interpretation. Der Sicherheitsmodul gewährleistet beispielsweise eine irreversible und somit sichere Schlüsselhaltung im hybriden Datenträger.

Anspruch 8 gewährleistet bei einer autorisierten Nutzung des Datenträgers einen raschen Datenzugriff. Die Operationen der Schreibe-/Lese-Einheiten für den hybriden Datenträger können unabhängig voneinander ausgeführt werden.

Gemäß Anspruch 9 sind die vorgenannten Schreib-/Lese-Einheiten miteinander logisch gekoppelt, was eine zusätzliche Sicherheitsmaßnahme gegen unautorisierte Nutzung des Datenträgers bedeutet. So kann z.B. die eine Schreib-/Lese-Einheit in einem geschützten Modus bleiben, wenn die andere Einheit mit keinem oder nicht mit dem richtigen Sicherheitsmodul kommuniziert. Die logische Kopplung der Schreib-/Lese-Einheiten ist entweder fest vorgegeben (geschlossenes System) oder kann von außen - reversibel oder irreversibel - eingebracht werden (offenes System).

Gemäß Anspruch 10 ist die Interaktionseinrichtung gewissermaßen als zusätzlicher Sicherheitsmodul ausgebildet. Bei einer unautorisierten softwaremäßigen oder hardwaremäßigen Manipulation werden entsprechende Steuersignale erzeugt, die eine logische Kopplung zwischen den Schreib-/Lese-Einheiten irreversibel zerstören.

Nach Anspruch 11 ist die Interaktionseinrichtung kompakt und platzsparend aufgebaut, wodurch die Montage der gesamten Schutzvorrichtung vereinfacht ist.

Die Erfindung wird anhand der in den Figuren dargestellten Ausführungsbeispiele näher erläutert. Darin zeigen:

Fig.1 einen hybriden Datenträger,

Fig.2 eine hybride Interaktionseinrichtung,

Fig.3 die funktionelle Kombination des hybriden Datenträgers gemäß Fig.1 mit der hybriden Interaktionseinrichtung gemäß Fig.2,

Fig.4 die Draufsicht auf einen herkömmlichen, als Diskette ausgebildeten Datenträger mit integriertem, kontaktbehafteten Sicherheitsmodul.

Fig.5 die Draufsicht auf einen als CD-ROM ausgebildeten Datenträger mit integriertem, kontaktlosen Sicherheitsmodul.

Die erfindungsgemäße Schutzvorrichtung enthält als wesentliche Bestandteile einen hybriden Datenträger 4 (Fig.1) und eine hybride Interaktionseinrichtung 5 (Fig.2). Der hybride Datenträger 4 besteht im wesentlichen aus einem transportablen und herkömmlichen Massenspeicher als Datenträger 1 und aus einem Sicherheitsmodul 2. Der Datenträger 1 und der Sicherheitsmodul 2 sind durch eine physikalische Kopplung 3 miteinander verbunden. Für einen Zugriff auf seine Daten kommuniziert der Datenträger 1 mit der über eine Schnittstelle 6 an einen Rechner angeschlossenen Interaktionseinrichtung 5 (Fig.3). Dabei wirken der Sicherheitsmodul 2 und die Interaktionseinrichtung 5 als Bestandteile der Schutzvorrichtung derart zusammen, daß nur in Abhängigkeit eines Austausches von aufeinander abgestimmten Informationen zwischen dem Sicherheitsmodul 2 und der Interaktionseinrichtung 5 auf die Daten des Datenträgers 1 und/oder auf die Interaktionseinrichtung 5 in einer für einen Benutzer auswertbaren Form zugreifbar ist.

Als Datenträger 1 sind sämtliche herkömmlichen Massenspeicher einsetzbar, z.B. eine Diskette mit integriertem, kontaktbehafteten Sicherheitsmodul 2 (Fig.4) oder eine CD-ROM mit integriertem, kontaktlosen Sicherheitsmodul (Fig.5).

Die physikalische Kopplung 3 ist je nach Anwendungsfall fest, schwer lösbar oder lose ausgebildet. Der Sicherheitsmodul 2 ist zu seiner physikalischen Kopplung 3 in den Datenträger 1 bzw. in dessen Gehäuse eingelassen, implantiert oder auf den Datenträger 1 aufgesetzt. Der Sicherheitsmodul 2 kann auch Bestandteil des Datenträgers 1 selbst sein. Die physikalische Kopplung 3 ist durch eine logische Kopplung zwischen Datenträger 1 und Sicherheitsmodul 2 ergänzt. Hierzu enthält der Sicherheitsmodul 2 einen integrierten Halbleiterschaltkreis bzw. besteht aus einem solchen Halbleiterschaltkreis.

Der Sicherheitsmodul 2 enthält einen Kryptoprozessor bzw. besteht aus einem Kryptoprozessor. Die Daten sind dann auf dem Datenträger 1 verschlüsselt abgelegt und können nur im Zusammenwirken mit der dafür vorgesehenen hybriden Interaktionseinrichtung 5 genutzt, d.h. in einer für den Benutzer auswertbaren Form entschlüsselt werden. Zwar können die verschlüsselten Daten in der Regel mit einem herkömmlichen Lesegerät für den jeweiligen Datenträger-Typ ausgelesen werden, mit dem Inhalt der Daten kann aber kein unautorisierter Benutzer etwas anfangen, da durch den Verschlüsselungsschutz die Datennutzung ausgeschlossen ist.

Die Interaktionseinrichtung 5 weist für den Datenträger 1 und für den Sicherheitsmodul 2 jeweils eine Schreib-/Lese-Einheit auf (Fig.3). Die Schreib-/Lese-Einheiten der Interaktionseinrichtung können derart miteinander logisch gekoppelt sein, daß die logische Kopplung die Operationen der Schreib-/Lese-Einheiten bestimmt. Die Interaktionseinrichtung 5 kann auch derart ausgebildet sein, daß die logische Kopplung zwischen den Schreib-/Lese-Einheiten bei einer unautorisierten softwaremäßigen oder hardwaremäßigen Manipulation irreversibel zerstört wird. In diesem Fall wirkt die Interaktionseinrichtung 5 als Sicherheitssystem. In Fig.3 ist die Interaktionseinrichtung 5 als eine einzige physikalische Einheit ausgebildet.

Die Interaktionseinrichtung 5 (siehe Fig. 2) dient - wie bereits gesagt - dazu, mit dem Datenträger 1, dem Sicherheitsmodul 2 und mit der Umwelt - z.B. einem Rechner - über die Schnittstellen 6,7,8 zu kommunizieren . Diese Kommunikation kann offen oder durch den Sicherheitsmodul 2 geschützt sein. Die Eigenschaften der Interaktionseinrichtung 5 können frei festgelegt werden, z.B. für Sicherheitsanwendungen. Die Interaktionseinrichtung 5 kann als offenes oder geschlossenes System oder als Sicherheitssystem ausgeführt sein.

Die Kommunikation über die Schnittstelle 8 zwischen dem Datenträger 1 und der Interaktionseinrichtung 5 findet auf die datenträgerspezifische Weise (optisch, elektromagnetisch, galvanisch etc.) statt.

Die Kommunikation über die Schnittstelle 7 zwischen dem Sicherheitsmodul 2 und seiner Interaktionseinrichtung 5 findet modulspezifisch (optisch, elektromagnetisch, galvanisch etc.) statt.

Der Zugriff auf die durch die Daten repräsentierte Information kann nur in Kooperation mit der Interaktionseinrichtung 5 erfolgen. Dies kann etwa durch Verschlüsselung, PIN-Schutz und/oder sichere Schlüsselhaltung im Sicherheitsmodul 2 realisiert sein.

Außerdem kann der Informationsgehalt des Datenträgers 1 nicht ohne Initialisierung des Sicherheitsmoduls 2 rekonstruiert werden. Beispielsweise wird die in Lohnherstellung bereitgestellte Software verschlüsselt auf CD (CD entspricht dem Datenträger 1) gepreßt, die Aktivierung erfolgt zu einem späteren Zeitpunkt durch den Softwarehersteller selbst. Dadurch wird der zunächst anonyme Datenträger 1 eindeutig identifizierbar und die Information wird erst dadurch nutzbar gemacht.

Dadurch ist man in der Lage, Vertraulichkeit, Authentizität, Verbindlichkeit, Originalität, Anonymität und sonstige Sicherheitsanforderungen zu realisieren.

Der typische Fall einer kombinierten Anwendung ist die gegenseitige Authentifikation von hybridem Datenträger 4 mit einer Interaktionseinrichtung 5 dadurch, daß zwischen der als Sicherheitseinrichtung ausgebildeten Interaktionseinrichtung 5 und dem Sicherheitsmodul 2 auf dem Datenträger 1 Authentifikationsprotokolle ausgeführt werden. Zu diesem Zweck können der Sicherheitsmodul 2 und die Interaktionseinrichtung 5 derart ausgebildet sein, daß sie in der Lage sind, Schlüssel vertraulich aufzubewahren und Daten weiterzuverarbeiten.

Hierzu ist der Sicherheitsmodul 2 z.B. als Mikrocontroller oder Kryptocontroller ausgebildet, während auf der Seite der Interaktionseinrichtung 5 ein Mikrocontroller, Krypto- oder Signalprozessor oder ähnliches eingesetzt wird. Weil auf der Interaktionsseite keine Restriktionen hinsichtlich Platz und Leistung bestehen, sind dort der Ausgestaltung keine Grenzen gesetzt. Die vertraulichen Informationen und Algorithmen können über die Schnittstelle 6 geladen werden oder sind bereits im hybriden Datenträger 4 bzw. im Sicherheitsmodul 2 unverändert hinterlegt.

Kombinationsanwendungen sind (personalisiert und unpersonalisiert) möglich. Die Interaktionseinrichtung 5 kann auch für die Zusammenarbeit nur mit dafür speziell konfigurierten Datenträgern 4 bestimmt sein.

Die Interaktionseinrichtung 5 kann Daten verknüpfen, kanalisieren und als Weiche operieren. Dadurch bestimmt die Interaktionseinrichtung 5 den Umfang des Umformens, Auswertens, Schreibens und Lesens der Daten des Datenträgers 1.

Bezugszeichenliste

1	Datenträger
2	Sicherheitsmodul
3	physikalische Kopplung
4	hybrider Datenträger
5	hybride Interaktionseinrichtung
6	Schnittstelle
7	Schnittstelle
8	Schnittstelle

Ansprüche

1. Vorrichtung zum Schutz
   - eines transportablen Speichermediums, insbesondere Massenspeichers als Datenträger (1) und/oder
   - einer für die Datennutzung des Datenträgers (1) mit ihm kommunizierenden und an eine Datenverarbeitungseinheit, z.B. an ein Rechnersystem anschließbaren Interaktionseinrichtung (5)

   gegen unerlaubte Nutzung,

   dadurch gekennzeichnet,
   - daß der Datenträger (1) mit mindestens einem Sicherheitsmodul (2) physikalisch gekoppelt (3) ist und
   - daß der Sicherheitsmodul (2) und die Interaktionseinrichtung (5) als Bestandteile der Schutzvorrichtung zusammenwirken derart,
   - daß nur in Abhängigkeit eines Austausches von zugehörigen, aufeinander abgestimmten Informationen zwischen dem Sicherheitsmodul (2) und der Interaktionseinrichtung (5) auf den Datenträger (1) und/oder auf die Interaktionseinrichtung (5) in einer für einen Benutzer auswertbaren Form zugreifbar ist.

2. Schutzvorrichtung nach Anspruch 1,

   gekennzeichnet durch

   eine feste oder zumindest schwer lösbare physikalische Kopplung (3) zwischen Datenträger (1) und Sicherheitsmodul (2).

3. Schutzvorrichtung nach Anspruch 1,

   gekennzeichnet durch

   eine lose physikalische Kopplung (3) zwischen Datenträger (1) und Sicherheitsmodul (2).

4. Schutzvorrichtung nach einem der Ansprüche 1-3,

   dadurch gekennzeichnet,

   daß der Sicherheitsmodul (2) zur physikalischen Kopplung (3) in den Datenträger (1) implantiert oder auf den Datenträger (1) aufgesetzt ist.

5. Schutzvorrichtung nach einem oder mehreren der vorhergehenden Ansprüche, gekennzeichnet durch
eine logische Kopplung zwischen Datenträger (1) und Sicherheitsmodul (2).

6. Schutzvorrichtung nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet,
daß der Sicherheitsmodul (2) einen integrierten Halbleiterschaltkreis enthält, insbesondere aus einem integrierten Halbleiterschaltkreis besteht, wobei dieser Schaltkreis mit der Interaktionseinrichtung (5), insbesondere mit einem in der Interaktionseinrichtung (5) eingebauten integrierten Halbleiterschaltkreis zusammenwirkt.

7. Schutzvorrichtung nach Anspruch 6, dadurch gekennzeichnet,
daß der Sicherheitsmodul (2) und/oder die Interaktionseinrichtung (5) einen Kryptoprozessor enthält.

8. Schutzvorrichtung nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet,
daß die Interaktionseinrichtung (5) jeweils eine Schreib-/Lese-Einheit für den Datenträger (1) und für den mindestens einen Sicherheitsmodul (2) aufweist.

9. Schutzvorrichtung nach Anspruch 8, dadurch gekennzeichnet,
- daß die Schreib-/Lese-Einheiten der Interaktionseinrichtung (5) miteinander logisch gekoppelt sind und
- daß die logische Kopplung die Operationen der Schreib-/Lese-Einheiten bestimmt.

10. Schutzvorrichtung nach Anspruch 9, dadurch gekennzeichnet,
daß die Interaktionseinrichtung (5) derart ausgebildet ist, daß die logische Kopplung bei einer unautorisierten Manipulation irreversibel zerstört wird.

11. Schutzvorrichtung nach einem der Ansprüche 8-10, dadurch gekennzeichnet,
daß die Interaktionseinrichtung (5) eine einzige physikalische Einheit ist.

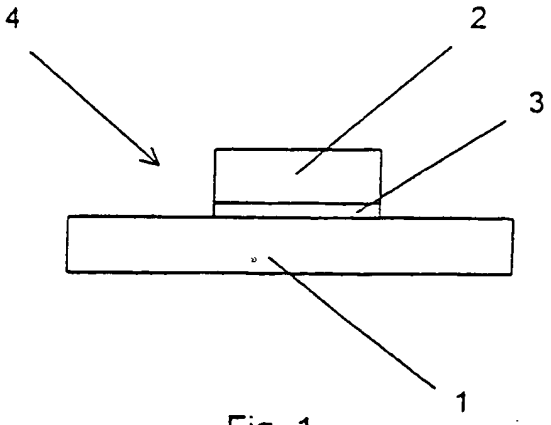


Fig. 1

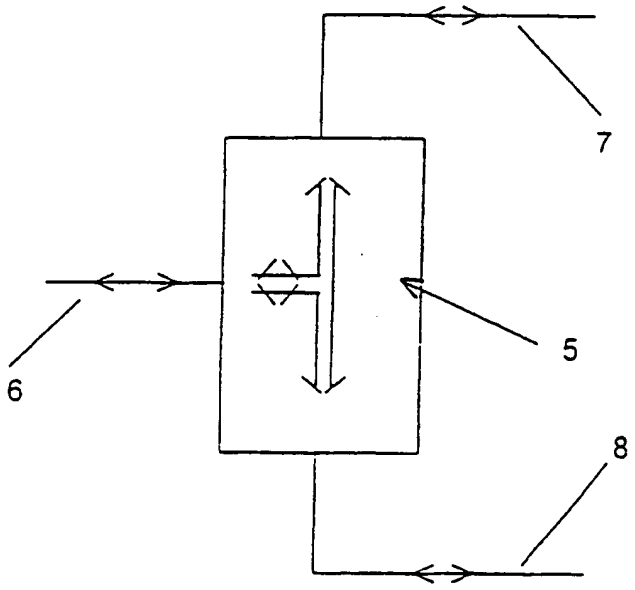


Fig. 2

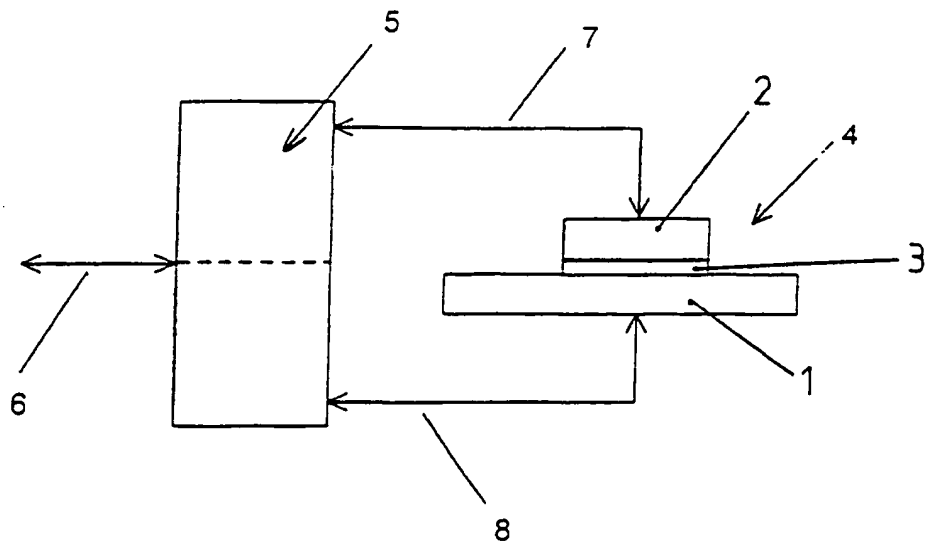


Fig. 3

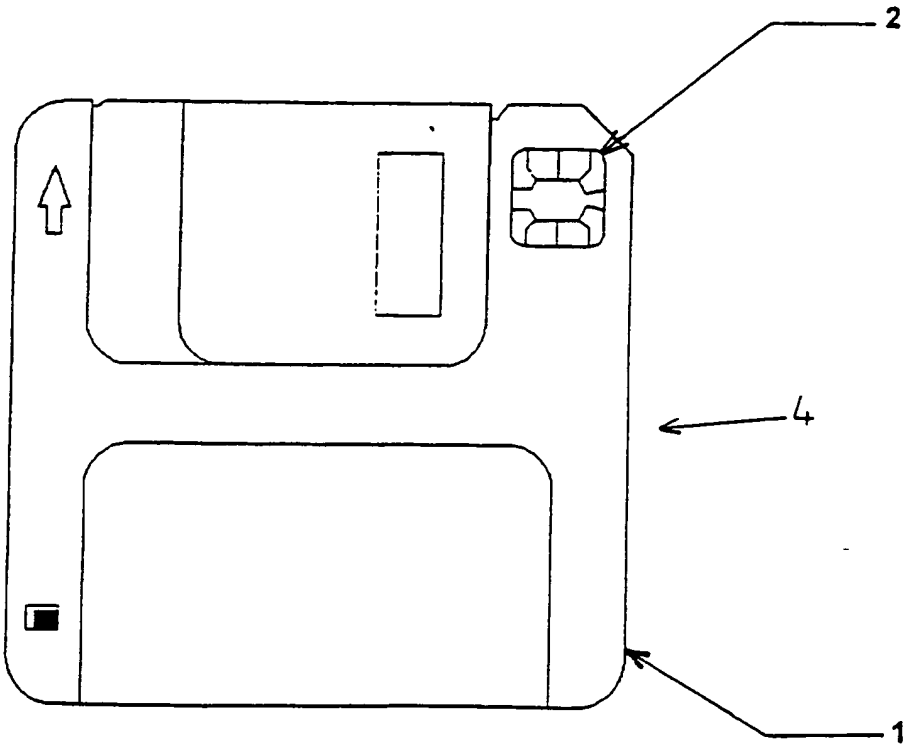


Fig. 4

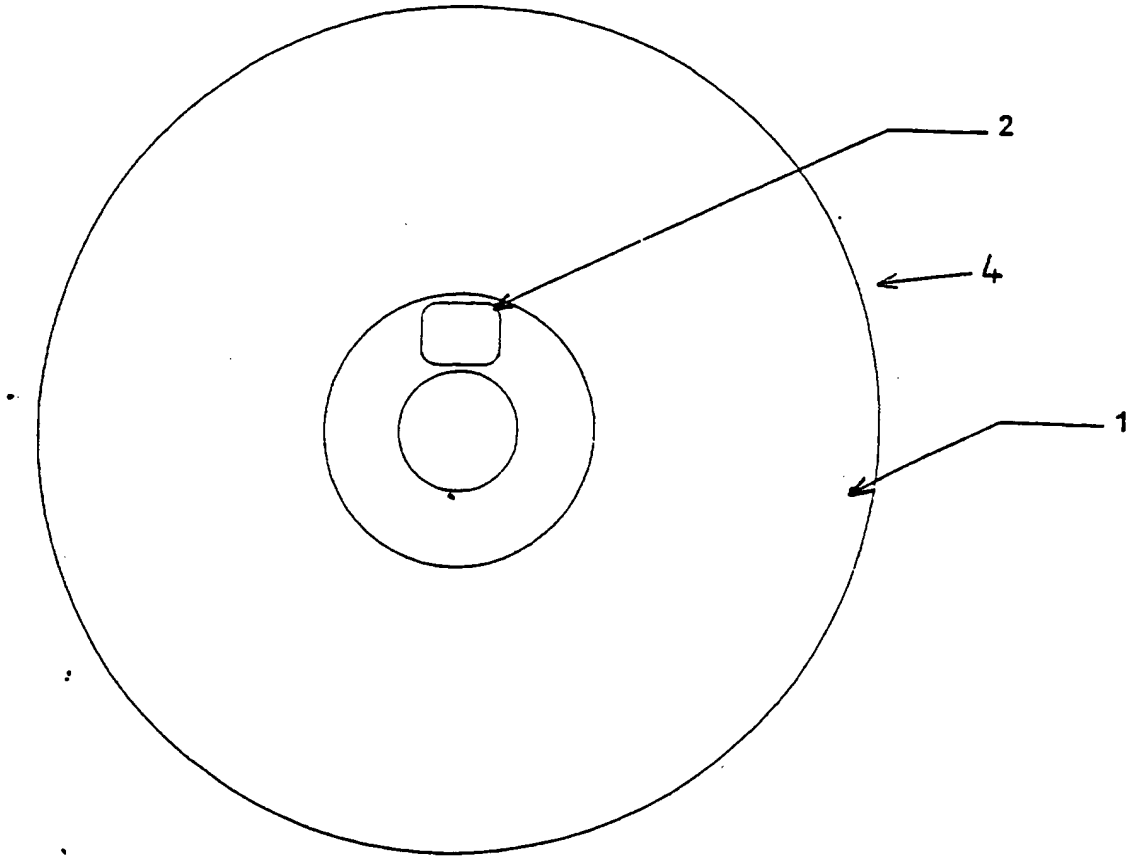


Fig. 5

INTERNATIONAL SEARCH REPORT

Interr ial Application No
PCT/EP 96/01175

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G11B20/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G11B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO,A,89 12890 (DUPRE MICHEL JEAN) 28 December 1989 see abstract; claims 1-7	1,2,5-9
X	FR,A,2 643 475 (LIVOWSKY JEAN MICHEL) 24 August 1990 see abstract; claims 1-13	1,2,5,6, 8,9
X	EP,A,0 600 660 (NINTENDO CO LTD) 8 June 1994 see column 2, line 32 - column 5, line 38 see column 6, line 9 - column 9, line 7; figures 2,3	1,3,5,6, 8,9
X	WO,A,90 06579 (VERNOIS GOULVEN JEAN ALAIN) 14 June 1990 see abstract see page 12, line 21 - page 14, line 34	1,2,5,6, 8,9

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 June 1996	18. 07. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Annibal, P

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO,A,90 06579 (VERNOIS GOULVEN JEAN ALAIN) 14.Juni 1990 siehe Zusammenfassung siehe Seite 12, Zeile 21 - Seite 14, Zeile 34	1,2,5,6, 8,9
X	EP,A,0 565 281 (NHK SPRING CO LTD) 13.Oktober 1993 siehe das ganze Dokument	1,2,5
A		3,7-9
X	US,A,4 910 625 (ALBRECHT FREDERICK X ET AL) 20.März 1990 siehe das ganze Dokument	1,2,4

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internales Aktenzeichen
PCT/EP 96/01175

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO-A-8912890	28-12-89	FR-A-	2633086	22-12-89
FR-A-2643475	24-08-90	AU-B-	5173790	26-09-90
		WO-A-	9010292	07-09-90
		GR-A-	90100111	28-06-91
EP-A-0600660	08-06-94	JP-A-	6161902	10-06-94
		AU-B-	666232	01-02-96
		AU-B-	5187993	09-06-94
		BR-A-	9304810	14-06-94
		CA-A-	2109982	27-05-94
		CN-A-	1117181	21-02-96
WO-A-9006579	14-06-90	FR-A-	2639755	01-06-90
		FR-A-	2647937	07-12-90
		AU-B-	4756190	26-06-90
		EP-A-	0446261	18-09-91
EP-A-0565281	13-10-93	JP-A-	5289612	05-11-93
US-A-4910625	20-03-90	KEINE		